Preface

This guide teaches you how to connect Milesight devices to the Milesight DeviceHub, and how to manage the devices on the Milesight DeviceHub.

Readers

This guide is intended for the following users:
- Distributors
- Network Planners
- On-site technical support and maintenance personnel
- Network administrators responsible for network configuration and maintenance

Copyright © 2011-2022 Milesight. All rights reserved.
All information in this guide is protected by copyright law. Whereby, no organization or individual shall copy or reproduce the whole or part of this user guide by any means without written authorization from Xiamen Milesight IoT Co., Ltd.

For assistance, please contact
Milesight technical support:
Email: iod.support@milesight.com
Tel: 86-592-5085280
Fax: 86-592-5023065
Address: Building C09, Software Park III, Xiamen 361024, China

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Doc Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug. 29, 2018</td>
<td>V 1.0</td>
<td>Initial version</td>
</tr>
<tr>
<td>Mar. 17, 2021</td>
<td>V 2.0</td>
<td>Brand Replace and add features</td>
</tr>
<tr>
<td>July 7, 2022</td>
<td>V 2.1</td>
<td>UG gateways support upgrade and provisioning in batches</td>
</tr>
</tbody>
</table>
# Contents

**Introduction** ........................................................................................................................................ 4

Compatibility ................................................................................................................................. 4

**Getting Started** ........................................................................................................................................ 4

Login DeviceHub ........................................................................................................................................................ 4

Account Options ...................................................................................................................................................... 5

Web Configuration Panel ...................................................................................................................................... 5

**Dashboard** ..................................................................................................................................................... 6

**Settings** .............................................................................................................................................................. 7

General Settings ....................................................................................................................................................... 7

User Management ...................................................................................................................................................... 9

Security Settings ....................................................................................................................................................... 11

Email Settings ............................................................................................................................................................ 11

Domain Settings ....................................................................................................................................................... 12

**Device Management** ......................................................................................................................................... 12

My Device ................................................................................................................................................................. 12

Search Device ........................................................................................................................................................... 12

Add Device ............................................................................................................................................................... 13

Monitoring Device’s Location ................................................................................................................................. 17

Visit Device ............................................................................................................................................................ 18

Edit Device ............................................................................................................................................................... 20

Select Device Administrator ................................................................................................................................ 21

Delete Device .......................................................................................................................................................... 21

Upgrade Device ...................................................................................................................................................... 21

Provisioning .......................................................................................................................................................... 22

Device Group .......................................................................................................................................................... 23

User Device ............................................................................................................................................................. 24

**Alarm** ................................................................................................................................................................. 25

Alarm List ................................................................................................................................................................. 25

Alarm Settings ....................................................................................................................................................... 26

**Task** ................................................................................................................................................................. 27
Introduction

Milesight DeviceHub provides a high-efficiency, low maintenance solution to easily deploy Milesight IoT devices across multiple locations, reducing complexity and increasing productivity. Milesight offers following DeviceHub versions:

- **Cloud Version:** devicehub.milesight-iot.com
  (Contact Milesight IoT sales or click [here](#) to apply for DeviceHub Cloud platform account.)
- **On-Premises Version:** Download from Milesight IoT website and install referring to *DeviceHub Installation Guide*.

Compatibility

The following Milesight IoT products support remote management feature:

- UR Series Router
- UF 5G CPE/Dongle
- UG Series Gateway

Getting Started

Login DeviceHub

Type the DeviceHub address to visit the login page. Enter the account(email) and password, click “Login”.
Account Options

After logging in, click the account at the right-upper corner, and a dialog box will pop up.

- **Language:** change the web language.
- **Settings:** edit the account settings.
- **Logout:** click to log out the Milesight DeviceHub.

Web Configuration Panel

There are 6 main sections on the web configuration panel.
- **Dashboard**
  View my devices, recent alarms, device status, and device groups.
- **Device**
  Manage devices.
- **Alarm**
  Check device alarms, configure alarm settings, and manage the alarms.
- **Operation Log**
  Check operation log related to the concurrent account.
- **Settings**
  Edit account settings and manage users.
- **Task**
  Check task status for your devices.

### Dashboard

On the dashboard, you can check your devices status, devices’ recent alarms, and your device groups.

- **My Device**
  Display the number of major alarm devices, offline devices, online devices, and total devices.

  ![My Device](image)

- **Status**
  The graph shows your device number according to the time (0-24 hours).
  - **Red** line shows new abnormal device number in the past hours. If there are major alarms on the device, the device will be considered as an abnormal device.
  - **Gray** line shows the concurrent offline device number.
  - **Green** line shows concurrent online device number.
  - **Blue** line shows concurrent total device number.

  If you check the option “Include User Device”, the graph will show both your device number and your users’ device number.
◆ Recent Alarms
Display the recent alarms for your devices. This page shows at most 10 alarms. For more alarm information, click on top of the screen.

◆ Group
Display the created device groups and the device number in the groups.

Settings
Click on top of the screen to manage your account settings and manage users.

General Settings
- My Information
  Check your account role, managing devices and edit your account name. Maximum number of managing devices is 25 by default for on-premises version. Please refer to DeviceHub Installation Guide to learn the steps of expanding the number of managing devices.
- **Notification**
  Check the option “Send alarm to email”, and fill in the recipients’ or your email address. If an alarm occurs on your device, you will receive the notification email.

  ![My Information](image)

  ![Notification](image)

  Following settings are only supported by **on-premises version**:

  - **System Information**
    Check the on-premises program version and serial number.

  ![System Information](image)

  - **Network Configuration**
    Enable NAT mode and type the public IP address for DeviceHub access by Internet. Configure the interval for Milesight devices to report status. Cloud version is fixed as 60s.

  ![Network Configuration](image)
User Management

DeviceHub supports adding different roles of Milesight device management accounts for your for the device installers and technical supports.

There is only one root account and it can create Super Admins, Admin users and Basic Users.

Super Admins can create Admin users and Basic Users.

Admins can create Basic Users.

Basic Users have task-based permission, no permission to create users, usually for a technical support or installer.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Role</th>
<th>Root</th>
<th>Super Admin</th>
<th>Admin</th>
<th>Basic User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Manage My Device</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Manage User Device</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td>Alarm Settings</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Operation Logs</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Create Super Admin</td>
<td></td>
<td>√</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Create Admins</td>
<td></td>
<td>√</td>
<td>√</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Create Basic Users</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>×</td>
</tr>
</tbody>
</table>

Add New User

1. Go to “User” tab and click “Add” to add a new user.
2. Fill in the user’s email address and other information.
3. Specify the user role and manageable devices.
4. Click “Save and send activation email”, the DeviceHub system will send an activation email to the user’s email address.
5. After finishing registration according to activation email, users can log in Milesight DeviceHub to add and manage devices.

**Edit User**

Click 📝 to edit the user information. If the user account is not activated, you can click “send activation email” with new activation link to the user again.

**Delete User**

Click 🗑️ to delete a user. If the user has device(s) in his device list, you cannot delete the user.
Before deleting the user, you need to transfer the device(s) managing authority to other user’s first.

**How to transfer device managing authority?**

**Security Settings**

On the Security page, you can change your login password. We recommend that you set a robust password with lower cases, upper cases and numbers.

**Email Settings**

On the Email page, you can configure the outgoing email server or change the email information which you type when installation. This email address is used for sending sub-account activation emails and alarm emails. “Test” button is used to check the email server validation and save the setting automatically. This setting only work with root account under on-premises version.
Domain Settings

On the Domain page, you can add a custom domain name and upload your HTTP/HTTPS certificates. This setting only work with root account under on-premises version.

<table>
<thead>
<tr>
<th>General</th>
<th>User</th>
<th>Security</th>
<th>Email</th>
<th>Domain</th>
</tr>
</thead>
</table>

**Server Domain**

- Custom Domain
- Certificate
- Private Key

[Save] [Cancel]

Device Management

Click 🖼 on top of the screen to manage your devices and users’ devices.

My Device

On “My Device” page, you can manage devices, edit and change the devices’ administrator.

- The device is connected to DeviceHub and online.
- There is an alarm on the device; click the icon to check the alarm information.
- The device is offline or not connected to DeviceHub.

If the device becomes offline, you can’t access the device even if you click 🖼. And the icon will turn 🌚 in 10 minutes.

Search Device

You can search for device you want to operate by Device Name, Device Group, Serial Number, MAC address or Model.
Enter relevant information in the search field, click to search device from the device list.

Click to refresh the device list.

Click to choose which items to display.

Add Device

There are two ways to add devices to Milesight DeviceHub. Choose either of them to add devices according to your circumstance.

- Connect to Milesight DeviceHub via Account Info
- Connect to Milesight DeviceHub via Authentication Code

Connect to Milesight DeviceHub via Account Info

You can add your device to DeviceHub directly by account authentication.

1. Log in Web GUI of routers/gateways. After logging in, go to “System > Device Management”, and you will see the device management settings.

For UR Series Routers or UF 5G Products

![Device Management Interface](image)

Server Address

- **Cloud Version**: devicehub.milesight-iot.com
- **On-premises Version**: IP address or domain of the DeviceHub server, e.g. 220.82.63.79.
For UG Series Gateways

- **Cloud Version**
  
  **Activation Server Address**: devicehub.milesight-iot.com

  **Device Management Server Address**: https://devicehub.milesight-iot.com/acs

- **On-premises Version**
  
  **Activation Server Address**: IP address or domain of the DeviceHub server, e.g. 220.82.63.79.

  **Device Management Server Address**: http://<DeviceHub server address or domain>:8080/acs, e.g. http://220.82.63.79:8080/acs

2. Choose “Activation Method” as “By ID” or “By Account Name”, and fill in your DevicHub ID and password. For example:
3. Click “Connect”. If the device is connected to the Milesight DeviceHub, the status will show “Connected”.

![Device Management](image)

4. You can see the connected device appears on the My Device list of the DeviceHub, and the status shows “Connected”.

![Device List](image)

### Connecting to Milesight DeviceHub via Authentication Code

Device’s operator can connect the device to Milesight DeviceHub via authentication code assigned by the DeviceHub users.

**For the DeviceHub Users**

1. Click “Add”, enter a name to help yourself identify the device, and then click “Add”.

![Add Device](image)

2. Verify Serial Number and MAC address.
   - **Check the option**: you need to fill in the device’s Serial Number and Ethernet port MAC address. The generated authentication code is only applicable for the specific device.
Note: For UR routers or UF51, you can find the MAC address on web GUI "Status > Overview > WAN > MAC"; for UF31, you can find the MAC address on web GUI "Network > Interfaces > LAN"; for UG gateways, you can find the MAC address on "Packet Forwarder > General > Gateway EUI", the MAC address is gateway EUI removed "FFFE", example: the Gateway EUI is 24E124FFFE0E201, then the MAC address is: 24:E1:24:F0:E2:01.

- Uncheck the option: any router can connect to the DeviceHub via the randomly generated authentication code. Once the device is connected to the DeviceHub, the router’s Serial Number and MAC address will be automatically filled in.

3. Click “Add”, and the system will generate an authentication code.

![Device Added](image)

Add the device successfully.
Please input the code in device's Web Interface.

The code is:
MzE1Mzc4YWYwMGQ3NTA4NzIzWjM2MwYjk3NWFhNWM=

- Send Code to Email
- Copy Code

4. Send the code to the operator’s email or copy the code and send it to the operator.

For the device’s operator
5. Log in the device’s Web GUI. Go to "System > Device Management", and fill in the DeviceHub information referring last steps.

![Device Management](image)

6. Click “Connect”. If the code is correct, the status will show “Connected”.
Monitoring Device’s Location

This feature only apply for **UR series routers with GPS**. Before monitoring device’s location, log in router’s Web GUI, and go to “Industrial > GPS > GPS” to enable GPS function.

Go to “My Device” on DeviceHub and click 📍 to monitor the router’s location and historical route.
Visit Device

1. Log in web GUI of devices to enable remote HTTP/HTTPS services.
   For UR series routers, go to “Network > Firewall” to enable remote access services.
For UG series gateways, go to “System > General Settings” to enable access services.

2. Click ☑️ and select the timeout value from the drop-down menu, then click “Visit”.

3. The system will give you an address to access the device, click on the URL to access the device.

If SSH is enabled, the dialog box will display as below.
4. After you log in the devices, you can view and manage configurations remotely.
5. Click the timeout in the device list, you can select “Extend the time” or “Force Quit Connection”.

**Edit Device**

Click ☑ to view and edit the device information. You can edit the device's name and assign the device to a group.
Select Device Administrator

Click to select the device administrator.

- If a user is selected, he/she can manage the device on the DeviceHub.
- If a user’s management authority is removed, the device will be deleted automatically from his/her device management account.

Delete Device

Click to delete a device from the device management. If the device is still connected, you need to click and select “Force Quit Connection” to quit device connection first. Then click to delete the device.

Note: If the device is managed by multiple users, and you delete the device, the device will also be deleted from other users’ device management accounts.

Upgrade Device

1. Select the devices you want to upgrade, and the devices should be of the same model, firmware and hardware, then click “Upgrade”.
2. Click “Select File” to upload the devices firmware file (firmware can be downloaded on Milesight
IoT website). After the firmware is uploaded successfully, you can click “save” to complete the upgrading. If you need to upgrade the offline devices, check “Offline Device Upgrade”, then DeviceHub will complete the upgrade after the devices are online. Note that if DeviceHub server or device network speed is slow, do not set the “Task Pending” as 0s.

3. You can view the upgrade task status by clicking .

Provisioning

1. Select the devices you want to synchronize the configuration, and the devices should be of the same model, firmware and hardware, then click “Provisioning”.

2. For UR routers and UF 5G products, click “Obtain” to obtain one device's configuration. The configuration information will be shown in the right textbox, then you can modify the parameters and click "Deploy" to send and apply the devices you have selected. If you want to deploy the off-line devices, check “Apply to Offline Device”.
3. For UG gateways, click "Select File" to upload the device .dat format configuration file (you can get the file on any gateway “Maintenance > Backup and Restore” page). After the file is uploaded successfully, you can click "save" to apply the configuration. If you want to deploy the off-line devices, check "Offline Device Configuration", then DeviceHub will apply the configuration after the devices are online.

4. You can view the task status by clicking ...

Device Group

You can group your devices by areas, device models or other purposes.
1. Click “Add” to add a device group.
2. Specify the group name, and then click “Add”.

www.milesight-iot.com
3. Click to edit the device group name, add or remove devices.

4. Click “Add” to add the devices into the group, then click “save”.

**User Device**

On the “User Device” page, you can check all your users’ devices.

- Select Users from the drop-down menu to check different users’ devices.
- Enter contents in the search field, click to search device from the device list.
- Click to choose which items to display.
- Click to select the device administrator.
The device is connected to Milesight DeviceHub.

The device is offline or not connected to Milesight DeviceHub.

Alarm

Click 🔔 on top of the screen to check alarm information for your managed devices and set the alarm settings.

Alarm List

When something is wrong with your device, an alarm message will be sent to Milesight DeviceHub. You can set the alarm events in Alarm Settings. You can search alarms by Alarm Level, Alarm Name, Time and device Serial Number.

Alarm Acknowledge

When the alarm appears, the device status will be displayed ● (red alarm). You should check the alarm information and fix the relevant issues for your device, then acknowledge the alarm.

1. Check the abnormal device and solve the problem.
2. Select the solved event from alarm list.
3. Click "Acknowledge".

www.milesight-iot.com
4. Your device status will be changed back to ● (green normal).

**Note:**
- If you don’t solve the device’s problem, and click “Acknowledge”, the device status will also turn to ● (green normal).
- If a device is managed by multiple users, all the users will receive the alarm information. If User A acknowledges the alarm, the device status on User B’s side will not be affected, it is still ● (red alarm).

**Alarm Settings**

On the “Alarm Settings” page, you can set which events to be recorded as alarms. There are two alarm levels, Major and Minor.

By default, Major Alarms are enabled. When the problems pop up, the alarm will be recorded on your Milesight DeviceHub account.

<table>
<thead>
<tr>
<th>Alarm List</th>
<th>Alarm Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Record</td>
</tr>
<tr>
<td>Device Disconnected</td>
<td>●</td>
</tr>
<tr>
<td>Device Deleted</td>
<td>●</td>
</tr>
<tr>
<td>Device Removed</td>
<td>●</td>
</tr>
<tr>
<td>System User Lockout</td>
<td>●</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device</th>
<th>Record</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cellular Down</td>
<td>●</td>
<td>Major</td>
</tr>
<tr>
<td>Failed to send SMS</td>
<td>●</td>
<td>Major</td>
</tr>
<tr>
<td>VPN Down</td>
<td>●</td>
<td>Major</td>
</tr>
<tr>
<td>WAN Down</td>
<td>●</td>
<td>Major</td>
</tr>
<tr>
<td>Cellular Up</td>
<td>●</td>
<td>Minor</td>
</tr>
<tr>
<td>Text messages received</td>
<td>●</td>
<td>Minor</td>
</tr>
<tr>
<td>VPN Up</td>
<td>●</td>
<td>Minor</td>
</tr>
<tr>
<td>WAN Up</td>
<td>●</td>
<td>Minor</td>
</tr>
</tbody>
</table>

**Operation Log**

Click 📊 on top of the screen to check operation logs for your account. On this page, you can check and search operation logs for Login, Logout, My Device, Remote Connection, Device Group, User Device, Alarm, General, User and Security executed by you and system administrator.
Task

Click 🕒 on top of the screen to check task status for your devices. On this page, you can check and search task for Upgrade, Configuration Obtaining and Configuration Deployment. Click “Start” to restart the failed or stopped tasks, click “Stop” to stop pending tasks.

-END-